IN THE CLAIMS:

Amended claims follow:

1. (Currently Amended) A computerized method comprising:

monitoring a peer-to-peer network for suspicious activity based on patterns of activity; and

performing an action associated with a suspicious pattern of activity when the suspicious pattern of activity is detected in the peer-to-peer network, the suspicious pattern of activity defined by a set of rules for detecting at least one of Trojan horse code, viruses, a user browsing data across peers, unwanted user activity, and malicious code attempting to contact a home location;

wherein the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network;

wherein the suspicious pattern of activity is defined in terms of a configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions in association with the shared data;

wherein monitoring a peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline.

2. (Original) The computerized method of claim 1, wherein monitoring a peer-to-peer network comprises:

evaluating network traffic among peers in the peer-to-peer network.

3. (Cancelled)

4. (Original) The computerized method of claim 1, wherein a pattern of activity is defined in terms of a threshold value of network traffic in the peer-to-peer network.

5. (Original) The computerized method of claim 1, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network that uses a specific protocol.

6. (Cancelled)

7. (Original) The computerized method of claim 1, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network having a foreign address.

8. (Cancelled)

9. (Previously Presented) The computerized method of claim 1, wherein the action comprises logging information about the suspicious pattern of activity.

10. (Previously Presented) The computerized method of claim 1, wherein the action comprises sending an alert about the suspicious pattern of activity.

11. (Original) The computerized method of claim 1, wherein the patterns of activity are local to a peer in the peer-to-peer network.

12. (Original) The computerized method of claim 1, wherein the patterns of activity are global to the peer-to-peer network.

13. (Currently Amended) The computerized method of claim 1 ~~further comprising:~~ ~~obtaining a~~wherein the set of rules ~~specifying~~specifies the patterns of activity as suspicious activity and specifies associated actions.

14. (Currently Amended) The computerized method of claim 13 further comprising:

refreshing the set of rules when the set of rules changes.

15. (Currently Amended) A computer-readable medium having executable instructions to cause a processor to perform a method comprising:

monitoring a peer-to-peer network for suspicious activity based on patterns of activity; and

performing an action associated with a suspicious pattern of activity when the suspicious pattern of activity is detected in the peer-to-peer network, the suspicious pattern of activity defined by a set of rules for detecting at least one of Trojan horse code, viruses, a user browsing data across peers, unwanted user activity, and malicious code attempting to contact a home location;

wherein the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network;

wherein the computer program product is operable such that the suspicious pattern of activity is defined in terms of a configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions in association with the shared data;

wherein the computer program product is operable such that monitoring a peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline.

16. (Original) The computer-readable medium of claim 15, wherein the method further comprises:

evaluating network traffic among peers in the peer-to-peer network when monitoring the peer-to-peer network.

17. (Cancelled)

18. (Original) The computer-readable medium of claim 15, wherein a pattern of activity is defined in terms of a threshold value of network traffic in the peer-to-peer network.

19. (Original) The computer-readable medium of claim 15, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network that uses a specific protocol.

20. (Cancelled)

21. (Original) The computer-readable medium of claim 15, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network having a foreign address.

22. (Cancelled)

23. (Previously Presented) The computer-readable medium of claim 15, wherein the action comprises logging information about the suspicious pattern of activity.

24. (Previously Presented) The computer-readable medium of claim 15, wherein the action comprises sending an alert about the suspicious pattern of activity.

25. (Original) The computer-readable medium of claim 15, wherein the patterns of activity are local to a peer in the peer-to-peer network.

26. (Original) The computer-readable medium of claim 15, wherein the patterns of activity are global to the peer-to-peer network.

27. (Currently Amended) The computer-readable medium of claim 15, wherein ~~the method further comprises:~~

~~obtaining a~~the set of rules ~~specifying~~specifies the patterns of activity as suspicious activity and specifies associated actions.

28. (Original) The computer-readable medium of claim 27, wherein the method further comprises:

refreshing the set of rules when the set of rules changes.

29. (Currently Amended) A system comprising:

a processor coupled to a memory through a bus;

a network interface coupled to the processor through the bus and further operable to selectively couple to a peer-to-peer network; and

a peer-to-peer security process executed by the processor from the memory to cause the processor to monitor the peer-to-peer network for suspicious activity based on patterns of activity, and to perform an action associated with a suspicious pattern of activity when the suspicious pattern of activity is detected in the peer-to-peer network, the suspicious pattern of activity defined by a set of rules for detecting at least one of Trojan horse code, viruses, a user

browsing data across peers, unwanted user activity, and malicious code attempting to contact a home location;

wherein the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network;

wherein the system is operable such that the suspicious pattern of activity is defined in terms of a configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions in association with the shared data;

wherein the system is operable such that monitoring a peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline.

30. (Original) The system of claim 29, wherein peer-to-peer security process further causes the processor to evaluate network traffic between the peers in the peer-to-peer network when monitoring the peer-to-peer network.

31. (Cancelled)

32. (Original) The system of claim 29, wherein the peer-to-peer security process further causes the processor to monitor the peer-to-peer network for a pattern of activity defined in terms of a threshold value of network traffic in the peer-to-peer network.

33. (Original) The system of claim 29, wherein the peer-to-peer security process further causes the processor to monitor the peer-to-peer network for a pattern of activity defined in terms of network traffic in the peer-to-peer network that uses a specific protocol.

34. (Cancelled)

35. (Original) The system of claim 29, wherein the peer-to-peer security process further causes the processor to monitor the peer-to-peer network for a pattern of activity defined in terms of network traffic having a foreign address.

36. (Cancelled)

37. (Previously Presented) The system of claim 29, wherein the peer-to-peer security process further causes the processor to log information about the suspicious pattern of activity when performing the action associated with the suspicious pattern of activity.

38. (Previously Presented) The system of claim 29, wherein the peer-to-peer security process further causes the processor to send an alert about the suspicious pattern of activity when performing the action associated with the suspicious pattern of activity.

39. (Original) The system of claim 29, wherein the system is a peer in the peer-to-peer network and the patterns of activity are local to the system.

40. (Original) The system of claim 29, wherein the system is a server in the peer-to-peer network and the patterns of activity are global to the peer-to-peer network.

41. (Original) The system of claim 40, wherein the system is a border firewall.

42. (Original) The system of claim 40, wherein the system is a domain name server.

43. (Currently Amended) The system of claim 29, wherein the ~~peer-to-peer security process further causes the processor to obtain a~~ set of rules ~~specifying~~specifies the patterns of activity as suspicious activity and specifies associated actions.

44. (Original) The system of claim 43, wherein the peer-to-peer security process further causes the processor to refresh the set of rules when the set of rules changes.

45. (Previously Presented) The computerized method of claim 1, wherein a share configuration loop is executed to detect changes to shares and corresponding permissions, and an action is initiated as a function of a type of the changes.

46. (Previously Presented) The computerized method of claim 45, wherein the share configuration loop is executed dynamically.

47. (Previously Presented) The computerized method of claim 45, wherein the share configuration loop is executed on a schedule.

48. (Previously Presented) The computerized method of claim 45, wherein the share configuration loop examines a current share configuration against a previously recorded shared configuration to detect the changes to the shares and the corresponding permissions.

49. (Previously Presented) The computerized method of claim 45, wherein, if the change includes an attempt to un-share a file or directory, the action includes a log entry.

50. (New) The computerized method of claim 1, wherein the suspicious pattern of activity includes a number of failed attempts by a computer in accessing an internal peer that exceeds a predetermined number.

51. (New) The computerized method of claim 1, wherein the suspicious pattern of activity includes more than a pre-defined number of internal computers requesting resolution of a single external address within a preset period of time.

52. (New) The computerized method of claim 45, wherein the share configuration loop is executed in parallel with a network traffic loop that detects incoming or outgoing network traffic from a computer as exhibiting an activity pattern defined as suspicious by a rule.